Preventing Policy Breaches

Michael Barwise

In my experience, the greatest contributor to breached policies is poor quality policies. What most businesses call "policies" are often ineffective because they get in the way of doing business, address the wrong problem or are vague or ambiguous.

Policies should not in any case be end-user documents. They should inform procedures that integrate closely with business processes. That means that although the policy may be universal, the procedures it informs will vary according to the activities of different business processes. The objective is to ensure that the security objective (not "the policy" but what the policy is aimed at achieving) is transparently fulfilled in the normal course of business activities without staff having to think about security independently of the task in hand. While security objectives remain externalities to day-to-day operations they will inevitably breached, as the immediate demands of business must come first. The ideal is that people carry out intrinsically robust business procedures without having to think whether they are fulfilling security objectives.

Effective compliance also demands a much more equitable sharing of security responsibilities between the technical and non-technical echelons than is commonly found in either business or the public sector. All too commonly, non-technical end users are provided with insecure systems and instructed to use them in a secure manner - effectively passing the whole and sole responsibility for endpoint security to those least equipped to manage it. On top of which they are frequently asked to perform their duties in a way that forces them to break the essence, if not the letter, of the rules they have been given in "policies".

So rather than starting from sacking people for not following incompetently created policies that intrinsically fail to fulfil security objectives effectively, we should first improve the quality and efficacy of policy development. That requires intelligent analysis of business-level security threats right down to first principles and synthesis from those first principles of robust solutions using a balanced and proportionate mix of technologies, procedures and business process re-engineering. All three must mesh to provide a coherent, well-directed defensive policy. Only then can effective procedures be defined, taking into account the primary purpose - to conduct business.

Originally appeared on LinkedIn, January 2012